1.1.1.) Principles relating to processing of personal data

This section provides clarity and guidance on the principles for processing data lawfully. The lawful processing of data is a fundamental principle that must be adhered to. When assessing the processing, importance should be placed on analyzing the processing as a whole rather than reviewing individual details. Chapter 2 (Art. 5-11) of the GDPR contains rules governing the processing of personal data. Art. 5 and 6 contain general requirements for the processing of personal data. Art. 10, on the other hand, regulates the processing of personal data relating to criminal convictions and offences.

Before any personal data is processed it has to be ensured that the requirements of Art. 5 GDPR are met. In particular, Art. 5 GDPR specifies that the following principles of data processing must be met: lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; availability; integrity and confidentiality.

a) Lawfulness

Operators must ensure that the processing is lawful by ensuring compliance with at least one of the six principles in Art. 6 GDPR[1]. In short, operators must identify valid grounds for collecting and processing data. An example is to hold personal data to comply with legal requirements. It should be noted that multiple grounds may exist for one purpose and an operator should analyse the processing carefully before ultimately deciding on the legal ground for the specific processing.

b) Fairness

Fairness refers to the responsibilities of operators to only use personal data in a way that is fair. This means that data must not be processed in a way that is unexpected, misleading or unduly detrimental to the player concerned.

c) Transparency

Transparent processing is about being clear, open and honest about the processing and is linked to fairness. Transparency is always important but operators should be aware of the need to properly inform players before they enter into a relationship with them. This is achieved by making available a fair processing notice before allowing a player to finalise the account registration process.

Transparency also refers to the responsibilities of the data controller under Art. 12 GDPR, providing accurate, accessible and comprehensible information to players about the data collection, its scope and further use. In order to comply with this principle, lawful data processing has to be based on a valid legal basis.

It should be noted that the principle of transparency is subject to certain exceptions. Operators are allowed to not disclose to players certain information in cases in which the disclosure may affect, e.g., the prevention and detection of crime; the assessment or collection of a tax; trade secrets; all other situations in which the law provides an obligation of confidentiality. This is for example related to situation of different profiling operations that are used for AML and anti-fraud purposes. Here

[1] See 1.1.2 “Lawfulness of processing”.

operators cannot reveal the logic behind these profiling operations since that would enable players to bypass them.

Nonetheless, the above exceptions have limitations and the operator must be able to justify and document the reasons for relying on an exemption, for example by demonstrating how the provisions exempting them from transparency apply to them and by informing players of their reliance on those provisions, when this would not be prejudicial to the purpose(s) of those provisions.

d) Purpose Limitation

This is one of the most important principles of data protection. It is essential that a purpose is defined before processing personal data. This aims to ensure that operators are clear and open about the reasons for obtaining personal data and that what operators do with the data is in line with the reasonable expectations of the individuals concerned. Art. 5.1 (b) GDPR prescribes that personal data may only be processed for specified, explicit and legitimate purposes. Personal data may not be processed in any other way incompatible with the initial purpose(s).

Based on these criteria, the operator has to determine whether the purpose disclosed to the player is compatible with any further (new) use of the personal data. If the new purpose is compatible, a new lawful basis for the further processing is not needed. However, operators should remember that if they originally collected the data on the basis of consent, a fresh consent needs to be obtained if new purpose cannot fit within initial consent purpose, to ensure that the new processing is fair and lawful[2].

e) Data Minimization

The principle of data minimization requires that personal data is limited to what is necessary in relation to the purposes for which they are processed. Operators are required to have data retention framework. In short, an operator should identify the minimum amount of personal data needed to fulfil the identified purpose. Operators should hold that much information, but no more. When assessing specific data processing always ask the question: is this data really needed?

The accountability principle means that operators need to be able to demonstrate that appropriate processes exist to ensure that they only collect and hold the personal data needed.

f) Accuracy

It is the responsibility of the operator to ensure that personal data is accurate and, where necessary, kept up to date. While the operator is responsible in this aspect, players are required to inform the operator when their personal data has changed. An operator must take every reasonable step to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

g) Storage Limitation

Personal data will be kept in a form which permits identification of players for no longer than is necessary for the purposes for which the personal data are processed, as an example, legal requirements as Know Your Customer. Operators need to consider, and be able to justify, how long they keep personal data. This will depend on the purposes for holding the data. Operators therefore

[2] See chapter 1.2 “consent”.

need a retention policy in place. The retention policy should be detailed enough to outline the retention periods for each processing activity and take into consideration different jurisdictional requirements as well as local laws, including licencing requirements. For these reasons, the retention period shall be evaluated on a case by case basis.

Operators need to periodically review the data they hold, and erase or anonymize it when such data is no longer needed.

h) Integrity and confidentiality

Necessary technical and organizational measures must be taken to ensure adequate data security and integrity. These measures are intended to prevent unauthorized or unlawful processing, unavailability of the data or accidental loss, destruction or damage to data[3].

1.1.2) Lawfulness of processing

Processing is lawful only if and to the extent that at least one of the following applies:

- the player has given consent to the processing of his personal data for one or more specific purposes[4];
- processing is necessary for the performance of a contract to which the player is party or in order to take steps at the request of the player prior to entering into a contract (e.g. registration and providing the services);
- processing is necessary for compliance with a legal obligation to which the operator is subject (e.g. fraud or AML reasons);
- processing is necessary for the performance of a task carried out in the public interest (e.g. ethics, sport integrity, anti-cheating, match-fixing);
- processing is necessary for the purposes of the legitimate interests pursued by the operator or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the player which require protection of personal data (e.g. potential legal claims of customers, sport integrity, anti-cheating, match-fixing)[5].

The processing activities within parenthesis represent examples and all processing must be individually analysed by the operator.

1.2) Consent

[3] See chapter 1.9 “security controls”.
[4] See chapter 1.2 “consent”.
[5] See chapter 1.3 “legitimate interests”.

This chapter outlines the principal issues operators shall consider when using the player's consent as a legal ground for the processing of personal data.

The GDPR sets a high standard for consent, but the biggest change is what this means in practice for consent mechanisms, which is summarised below:

- Consent must be "*freely given, specific, informed and unambiguous*"[6].
- Clear affirmative action: consent must always be given through an active motion or declaration, e.g. it can be requested by using "unticked" opt-in boxes or similar active opt-in methods.
- Review: consent shall be understood as an ongoing and actively managed choice, and not simply a one-off compliance box to tick and file away. Consent must be subject to review and updated if necessary. Each operator shall establish their own review policy, however consent should not be kept, and therefore considered valid, for longer than four years, unless mandated by relevant legislation.
- Granular: where possible, operators shall offer granular opt-in options to consent separately to different types of processing.
- Documented: operators shall keep records of consent. Evidence must be kept of consent being given or withdrawn, when the consent was provided, how the consent was received or withdrawn and what information the player received at this stage (e.g. which version of the Privacy Policy or Fair Processing Notice).
- Named: operators shall name the organisation, brand, group of companies and any third parties who will be relying on the specific consent in a role of controller.
- Unbundled: consent requests must be separate from other terms and conditions. Consent shall not be a precondition of signing up to a service. For example, it is not necessary to market to a player, or use their personal data in a data mining exercise, in order to provide them with a betting account.
- Easy to withdraw: operators shall explain clearly how to withdraw consent and make it easy for players to do so. This means operators shall have simple and effective withdrawal mechanisms in place. Where processing is based on consent, the withdrawal of consent will also involve the personal data processed by processors or sub-processors in relation to the consent.

When consent is used as a legal basis for processing personal data, operators shall ensure players are able to withdraw consent at any time in a simple manner. The most common mechanisms for withdrawing consent are, for example:

- Marketing emails: where players opted-in to receive marketing emails, operators will use their email address for this activity. If players no longer wish to receive marketing emails, they can use the unsubscribe link at the bottom of each marketing email;
- Marketing SMS messages: texting 'STOP' to a number given in the text message;
- Preference management centre: players can sign in to their accounts and withdraw their consent by visiting their preference centre;
- Settings tab for deactivating cookies.

[6] Recital 32 GDPR.

Operators adhering to the Code, shall refrain from using the following mechanisms:

- Pre-ticked boxes: pre-ticked opt-in boxes and other forms of consent by default. The SAs' guidance makes it clear that a consent obtained by failure to opt-out is not an admissible consent and such consent shall not be assumed by the operators. Operators shall provide granular options to consent separately for different types of processing wherever appropriate such as marketing cookies, analytic cookies and other type of cookies, as appropriate.
- Not bundled with terms and conditions: players shall not be prejudiced if they do not consent to certain processing of personal data.
- Confusing language: e.g. double negatives or inconsistent language that is likely to confuse individuals.
- Disruptive mechanisms: consent mechanisms that are unnecessarily disruptive and repetitive to the players. The consent mechanisms shall be user friendly and the request for consent shall be clearly visible.
- Vague or blanket consent: request for consent worded so vaguely that it does not provide clear and specific information about what players are consenting to and with which operator they are sharing the data with.

Operators may carry out practices that incentivise consent among their players in some circumstances. Incentives shall not penalise players who refuse to consent to receive marketing materials.

It is important to note that in some processing activities operator will process data collected by other data controllers based on its consent to share data with third parties for their own purposes. In such situations, the operator needs to ensure that its contracts with such partners are clear in regard to obligation of that party to obtain a valid consent in accordance with the applicable law before processing such third party data. Operator will not have an obligation to verify the validity of such consent.

a) Objectives

Operators shall focus on the following objectives to ensure compliance with the GDPR in relation to consent:

- Identify the purpose for collecting personal data and the respective personal data collection points;
- When operators rely on consent for processing personal data, assess whether operators need to make any changes in relation to: (i) the mechanisms used to obtain consent; (ii) what information was provided to the player; (iii) whether information on how to withdraw consent was provided;
- Ensure that a process to track consent is implemented, in view of demonstrating that the player consented to the processing. Date and time must be included for such processing when a new record is created. This is often referred to as a date and time stamp;
- Keep evidence of up to date and accurate records of consents and suppression lists of withdrawal of consent and requests to opt-out.

1.3) Legitimate Interest

This chapter provides clarity and guidance on the interpretation and application of the legitimate interest condition for processing under the GDPR.

Operators must have clear, documented and repeatable processes for all aspects of the legitimate interest assessment, though these may be applied only as far as required in each assessment. These processes must provide documentation evidence, which must be retained for a minimum defined period (to be determined by the operator), showing that due consideration was given to the balancing test and the interests of the player. The processes must cover all eventualities of the legitimate interest assessment including the player's right to object and the subsequent review in light of the specific circumstances of the player.

The legitimate interests can be an operator's own interest or the interests of third parties. They can include commercial interests, individual interests or broader societal considerations.

a) Legitimate Interest Assessment

Whilst the process of the legitimate interest assessment ('LIA') is not part of the Code, any implementation of it must contain the following information at a minimum. The process must also be version controlled and regularly reviewed[7].

1. A description of the methodology used in the LIA process, including any risk assessment methods applied;
2. The legitimate interest pursued by the operator in the personal data processing;
3. Precise details on the personal data which will form part of the processing;
4. A specific description of any processing that will be applied to personal data under this LIA. This must include:
   4.1. The nature of the processing;
   4.2. What will trigger, or has triggered, the processing to occur;
   4.3. For how long the processing will continue;
   4.4. Retention periods where not covered by existing company policies, or the criteria to determine them;
   4.5. Whether new technology is involved and, if so, details of that technology;
   4.6. Whether the processing is likely to results in a high risk to the rights and freedoms of players and, if so, details of those risks shall be highlighted;
5. An explanation of why the processing is necessary and proportionate to achieve the legitimate interest;
6. A description of why this processing is within the reasonable expectations of the player[8], or an explanation of the compelling reasons justifying the processing;

[7] See here a template of LIA: https://ico.org.uk/media/for-organisations/forms/2258435/gdpr-guidance-legitimate-interests-sample-lia-template.docx

[8] See Opinion 06/2014 of Art. 29 Data Protection Working Party on the '*Notion of legitimate interests of the data controller under Art. 7 of Directive 95/46/EC*', pag. 40.

7. Any mitigating controls that will be implemented to manage risks to the player;
8. How data minimisation has been achieved including specific consideration of whether it is possible to offer opt-out to players;
9. How any specific subset of personal data has been selected for this processing;
10. Any benefits to the players in relation to the processing;
11. Consideration of the player's interests, rights and freedoms;
12. A statement on the period at which the LIA will be reviewed and a recognition that a significant change will also trigger a review.

b) Examples of Possible Legitimate Interests

All of the following examples apply only where the processing of personal data is necessary to achieve the desired outcome. Where it is reasonably possible, bearing in mind all relevant factors of the situation, to achieve the outcome without using personal data, then a legitimate interest justification for processing will not apply.

This list is not exhaustive and none of the items on it apply without challenge. The standard processes must be followed in each specific case to assess the legitimate interest. However, in these examples there is an assumption that if any risks to the player can be adequately controlled the use of legitimate interests is likely to be valid.

- System testing;
- To support any, though not specifically stated in, regulatory and licencing requirements that operators need to comply with;
- Necessary for the protection of players in line with Responsible Gambling monitoring activities;
- Necessary for the operator to understand the use of its services, products or technology to make improvements in customer experience;
- Necessary to target direct marketing where such communication is permissible under EU or any other Member State legislation;
- Strictly necessary for the prevention of harm to the operator or to players, including but not limited to unlawful actions or actions in breach of the terms and conditions;
- Necessary to protect players and the operator from breaches of the terms and conditions or rules associated with any activity;
- Analytic profiling for marketing purposes where consent is not a mandatory condition of processing;
- Profiling, when it does not involve automated decision-making and when it does not produce legal, or similarly significant, effects concerning the player.

Marketing activities may fall within the legitimate interest lawful basis. This covers all electronic channels of communication, except those for which the legislation requires consent Players should be aware of this in order to be able to object.
Moreover, it should be mentioned that there can be situations where the customer did not opt out from marketing communication, but becomes inactive. In these cases, the operators agree that if a

customer does not opt out, they can keep sending marketing communications to inactive players (subject to the rules on retention periods).
Also, since most of the gambling operators have different brands and game of chance services in their portfolio, it is permissible to advertise and promote other brands from other affiliated companies, if the products and services are same or similar to the ones the customer uses (e.g. send marketing material to a casino user about poker games of affiliated company) as long as this is in compliance with regulatory and compliance requirements.

c) Accountability and Transparency

All legitimate interests must be communicated to the player when first establishing a relationship in compliance with the GDPR, within reasonable expectations of the players. A detailed focus on the operators' privacy policy is provided in chapter 1.4 "Data Subject Rights" of the Code.

1.4) Data Subject Rights

This chapter will identify the various rights individuals have under the GDPR. These rights can be found in Art. 13 to 18 and 20 to 22 GDPR.

It is important for operators to take these rights very seriously and respond to requests within the relevant deadline in order to avoid any issues with Supervisory Authorities (SAs). When handling these requests, it is crucial to bear in mind good customer service strategies as that will likely make dealing with the request easier and will reduce the likelihood of a complaint to the relevant SA.

Before responding to any request that requires personal data to be released a review of that information must be undertaken to ensure the personal data of others, confidential references or any other personal data which may be covered by an exemption that the operator has chosen to use is not included in the reply to the request.

a) What are the rights granted to data subjects?

The GDPR provides individuals with the following rights: right to be informed; right to access; right to rectification; right to erasure; right to restriction of processing; right to data portability; right to object; right not to be subjected to automated individual decision-making, including profiling.

b) Right to be informed

Under Art. 13 and 14 GDPR, players have the right to be informed about the collection and use of their personal data. In addition to the information provided to the player stemming from Art. 13(1), operators must inform players about the purposes for processing their personal data, the criteria or reasons for which the data is being retained and the recipients or categories of recipients with whom

their data will be shared. Operators must regularly review and, where necessary, update their privacy information.

However, information does not have to be provided when personal data is obtained from other sources if:

- The player already has the information. Operator may include a reference to the link with the source of the information, e.g. privacy notice;
- Providing the information to the data subjects would be impossible;
- Providing the information to the data subjects would involve a disproportionate effort;
- Providing the information to the data subjects would render impossible or seriously impair the achievement of the objectives of the processing;
- The operators are required by law to obtain or disclose the personal data; or
- The operators are subject to an obligation of professional secrecy regulated by law that covers personal data.

The right to be informed relates to the transparency principle in the GDPR and demands that information relating to the processing of their Personal Data is presented to players in a clear and concise manner.

As a general rule, operators present this information to users of services through the privacy policy, which is brought to the attention of the player during the registration process. Operators can also provide other information through other means, when requested by the player. The privacy policy also contains a description of the data subject's rights mentioned in this chapter. Operators should always communicate changes to the privacy policy if they include substantive modifications.

c) Right to access

Under Art. 15 GDPR, individuals have the right to access their personal data as well as receive other supplementary information. These requests are commonly referred to as Data Subject Access Requests ('DSARs') or Subject Access Requests ('SARs').

Operators may decide internally their process to verify players prior to responding. Players are only entitled to access their own personal data, therefore operators shall prevent the inappropriate disclosure of third party's personal data to the requestor. If the data of others is included in the same document, operators may redact the personal data of those who are not the individual requestor. Also, operators must be mindful that when responding to a SAR, they do not negatively affect other rights and that a range of exemptions may apply such as trade secrets, IP and other related issues and on a case by case basis trade notes or business decisions, or logic behind those decisions, to the right to access. Operators do not always need to provide all data, especially in cases where there are legal requirements that would be jeopardized with such action, as explained above in case of profiling for compliance-AML purposes.

If it is not clear what the player is requesting, it would be useful to quickly revert back to the player and ask them to clarify what exactly it is that the player is requesting. Seeking clarity on a request may also narrow the scope of the information that the player is looking for.

Every operator must have a log to record the requests received in order to identify relevant deadlines and to comply with the principle of accountability.

When providing the relevant information for a requestor, the GDPR includes a best practice recommendation that, where possible, operators should be able to provide remote access to a self-service system which would provide the individual with direct access to his information.

d) Right to rectification

Under Art. 16 GDPR, players have the right to have inaccurate personal data rectified. The Code interprets personal data as 'inaccurate' if it is incorrect or misleading as to any matter of fact.

If the operator is satisfied that the data in question is accurate, it should explain to the player its decision to maintain the information, create an audit trail of such decision and inform the player of their right to make a complaint to the relevant SA.

Operators shall inform third parties about the rectification of personal data if the operator has in fact transferred the player's data to third parties (e.g. regulatory bodies, suppliers, joint controllers), unless this proves to be impossible or involves a disproportionate effort.

e) Right to erasure

Under Art. 17 GDPR, players have the right to have their personal data erased. This is commonly known as the 'right to be forgotten'. It is crucial to note that this is not an absolute right and applies only in certain circumstances.

In the context of the online gambling industry, it is important to balance the rights of the players with the respective operator's obligations under other areas of law, such as those under relevant tax and gambling regulations, as well as potential legal claims as referenced above. The full list of the exemptions to this right can be found in Art. 17(3) GDPR. Highlighting these exemptions to the requestor in the acknowledgement for the request for erasure will help the requestor understand the operator's overriding legal obligations.

Operators shall inform third parties about the erasure of personal data if the organisation has in fact transferred the player's data to third parties, unless this proves to be impossible or involves a disproportionate effort.

f) Right to restrict processing

Under Art. 18 GDPR, players have the right to restrict the processing of their personal data in certain circumstances. This is not to be confused with the right to erasure as this particular right only limits the ways in which the operator can use their personal data.

Where the processing has been restricted, the personal data shall, with the exception of storage, only be processed with the player's consent or for certain other exemptions.

Operators must aim at implementing mechanisms in place that enable the restriction of certain types of data or for certain purposes if required.

An operator shall inform third parties about the restriction of personal data if it has in fact transferred the player's data to third parties, unless this proves to be impossible or involves a disproportionate effort.

g) Right to data portability

Under Art. 20 GDPR, players have the right to have an operator send their personal data to another data controller. The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. This right applies only to data for which the processing is based on consent or on a contract, where the processing is carried out by automated means and when the data has been provided by the player to the operator. The following data shall be considered to be comprised by the right to data portability according to the Code:

- Personal data submitted by the player upon registration;
- Personal data which the player passed on to the operator in the course of any dealings between player and operator;
- Personal data which was generated by the operator from observation of the player's activity (e. g. activity logs, history of website usage, etc.).

However, the right to data portability does not include personal data where the justification for processing is not consent or contract, for example data which is processed for legitimate interests or legal obligation. Exempt data may include, but is not limited to:

- Results of an algorithmic analysis of the player's gaming behavior;
- Player's profile kept by operators in the context of risk-management and financial regulations;
- Player's data processed as part of the operators' obligations to prevent and detect money laundering and financial crimes, and manipulation of sports competitions, where stipulated by law.

The right to data portability entitles a player to receive a copy of their personal data and/or have their personal data transmitted from one operator to another operator in a safe and secure way, without affecting the usability of the data. Operators may also consider utilizing a portal from which the Player can directly access and export this Personal Data at any time, doing so would meet the requirements of Data Portability.

In light of the principle of data minimization, it might be expedient that the disclosing operator directly contacts the receiving operator, to determine which types of data are required by the latter and which format is best suited. However, the decision to opt for this approach shall rest with the player and shall not affect the principal obligation of the operator to provide another operator with the full data set as described above.

The specific format of the transmission is not covered by the Code and shall be agreed on a case by case basis between the operators. However, the data shall be provided in a format that is:

- structured (the structural relation between elements is explicit in the way data is stored),
- commonly used (the format is widely-used and well established), and
- machine-readable (the format shall be automatically read and processed by a computer).

Operators shall have in place documented procedures, which can also form part of the policies and processes required by this chapter. These procedures shall contain at a minimum:

- the kind of structured, commonly used and machine-readable format of the transmission;
- the secure methods of the transmission.

h) Right to object

This right is firstly engaged where an operator has justified the processing of a player's data by Art. 6(1)(e) or (f). Art. 21 GDPR grants the player the right to object to the processing of their personal data. Operators shall balance the rights of players against any existing conflicting legitimate ground which overrides the rights of the players or in case the personal data concerned is needed for the establishment, exercise or defence of legal claims that the operator may have. It is up to the operators to demonstrate that there is an overriding legal or legitimate ground which exempts them from enabling the player to exercise their right to object.

An example of exercising these rights can come in the form of objecting to direct marketing. This is the only situation where objection is an absolute right and there are no exemptions to refuse the player from being removed from marketing requests. In all other situations a balancing test must be conducted.

The player's right to object shall be first communicated to the player at the time of them receiving the first communication from an operator (e.g. with the "subscribe here" links for marketing communications).

i) Right not to be subjected to automated individual decision-making including profiling

Art. 22 GDPR grants the player the right not to be subject to a decision solely made on automated decision-making basis. It should be noted that this right shall not apply if the decision:

- Is necessary for entering into, or performance of, a contract between the player and the operator (such as KYC profiling tools);
- Is authorised by the Union or Member State law to which the operator is subject to (such as Responsible gaming and Fraud-AML profiling tools);
- Is based on the player's explicit consent (marketing profiling).

However, operators, to the extent possible, must implement suitable measures to protect the players' rights and at a minimum offer human intervention in the decision-making process.

1.4.1) Automated Decision-Making and Profiling

As computer systems evolve, in both speed and their ability to model decision making practices, it becomes increasingly cost effective to automate certain key decisions. This provides benefits to both the operator and the player, including speed, repeatability and consistency. In a similar way profiling can be used for a variety of reasons, including tailoring website content to an individual's interests or ensuring that they only receive relevant information.

These systems also come with risks. Not all situations match a predetermined set of rules and if the system misidentifies the data subject, their interests, or their patterns of behaviour then any decision is fundamentally flawed.

To protect data subject rights, the GDPR requires controls around automated decision making and profiling. This chapter will discuss best practice in these areas. Other requirements such as lawful and fair processing are discussed in their relevant chapters[9]. The definitions of the terms automated decision-making and solely automated decision-making are included in the definitions of the Code, while profiling is already defined in Art. 4 GDPR.

a) Automated Decision-Making and Solely Automated Decision-Making

It is key to differentiate decisions that are automated from those which are solely automated. All relevant processes must be mapped out, documented and the risk must be assessed. Decisions that are solely automated pose the highest possibility of risk to individual data subjects. Where the lawful reason for processing is legitimate interest, the risk assessment and associated balancing act are critically important[10].

For any type of processing to class as automated rather than solely automated, there must be meaningful human involvement in the process. Furthermore, that human involvement must take place prior to the final decision. As an extreme example, if a person was employed to simply click "accept" on every recommendation a computer makes, this would still class as solely automated processing. Similarly, if a person is employed to review only cases the system identifies as high risk then all other decisions are being made through solely automated processing.

[9] See chapter 1.1.1 "Principles relating to processing of personal data" and 1.1.2 "Lawfulness of processing".
[10] See chapter 1.3 "legitimate interests".

b) Profiling

The concept of profiling is related, but not identical to, the notion of both automated and solely automated processing.

To fall within the definition of profiling, processing must:

- involve automated processing, but may also contain human elements;
- be carried out on personal data that may not be considered personal data per se but enables the evaluation of personal aspects of a player;
- have the objective of evaluating personal aspects of a player;

and usually, but not exclusively, involves the following elements:

- data collection;
- data analysis to identify patterns and correlations to other data;
- use the analysis to anticipate characteristics of a player or their behaviour.

All profiling operations must comply with the GDPR requirements in full. The following section highlights several specific considerations that must be included but it is not an exhaustive list.

c) Transparency

A core tenant of the GDPR is that processing must be transparent but the complex business algorithms and technology behind profiling and automated decision-making are often invisible, or at best opaque, to individuals.

All operators must clearly identify and explain when either activity is used on personal data, and communicate this transparently and in an easily accessible manner to all players. This can be done through a privacy policy or through a layered approach linked to the privacy policy. In any way it is achieved, compliance with this point must be easily demonstrable.

The information must contain, where relevant, a clear description that the data will be used for profiling or in automated decision-making. These are two separate processes which must be clearly identified including all associated rights that the player has. The right to object must be explicitly brought to the attention of the player and it must be presented separate from other information. This can be made in the same communication as long as the point is made independently.

Where any such processing is solely automated, players have a right to be provided with meaningful information about the logic of the decision process, the significance and envisaged consequences for the player and any rights specific to solely automated decisions (except where this is not feasible due to applicable laws as explained above for AML & Fraud profiling tools).

d) Fair

Automated decisions and profiling rely on algorithms, statistical correlations and various assumptions in order to work. These assumptions, or the data inferred from a correlation, are not always accurate. One should not feel that a scientific approach based on numbers is inherently fair, it could easily have been affected by unconscious bias on behalf of the creator, a flaw in the original research on which it was based, or something as simple as an inability for computers to understand context.

Even where the conclusion of the system is accurate it may not be fair to action that conclusion in a specific way.

Depending on the information it may also be possible to infer new categories of personal data which the player did not grant permission to process, and for which operators have no legitimate reason to process. Studies have shown that information such as political affiliations, sexual orientation, ethnic origin or religion can be inferred from limited and ostensibly unrelated data. A poorly implemented profiling algorithm could easily begin to identify new data where there is no justification to process it.

Any use of profiling or automated decision-making must be subject to a documented risk assessment. This analysis must be documented and reviewed regularly, specifically when there is a significant change.

e) Purpose Limitation

On many occasions it may seem useful and efficient to use personal data gathered for other reasons to support profiling or automated decision-making. Before this can be done the operator must carefully analyse the data, the original purposes that were communicated to the players and the intended new use of the data. To maintain compliance with the accountability principle, this analysis and any decisions based upon it must be documented and reviewed regularly, or on significant change.

f) Rights of the Data Subject Regarding Solely Automated Decisions

Whilst the GDPR data subject rights apply generally to all processing, there are specific additional rights targeting solely automated decision-making.

Furthermore, for the solely automated data processing activities to be captured by these specific rights, the decision must produce legal or similarly significantly effects for the player. It is not thought that administrative decisions such as opening an account, declining to open an account, applying limitations or restrictions to an account, or excluding a player normally produce legal or similarly significant effects but each case must be reviewed on its specific merits.

g) Not to Be Subject to Solely Automated Decisions

To review Art. 22 (1) GDPR in full it states [emphasis added]:

> "*The data subject shall have the right not to be subject to a decision based **solely** on automated processing, including profiling, which **produces legal effects** concerning him or her **or similarly significantly affects** him or her.*"

Guidance from the EDPB elaborates that unlike most other 'rights' under the GDPR this right does not have to be actively invoked by the data subject, rather this type of processing is generally unlawful:

> The term "right" in the provision does not mean that Art. 22(1) applies only when actively invoked by the data subject. Art. 22(1) establishes a general prohibition for decision-making based solely on automated processing[11].

Any processing which involves a solely automated decision, as defined above, poses a potentially high risk to the player and must have a full Data Protection Impact Assessment ('DPIA') carried out[12] and any identified risks appropriately mitigated. This DPIA must be documented and reviewed regularly, or upon any significant change to the processing. However, as explained above, where processing operations are based on law or public interest obligations, and the relevant Member State's data protection authority has not included such processing in the list of processing activities that require DPIA, operators are not obliged to conduct DPIAs for these kinds of activities, unless they consider it necessary.

[11] WP 29, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, pag. 19.
[12] See chapter 1.11 "Processing requiring Data Protection Impact Assessments".

The general prohibition on solely automated decision-making means that any such processing must rely on an exemption listed in Art. 22. As part of the DPIA, the operator must clearly identify which exemption they are using to lawfully process the data, without this any processing is unlawful.

Art. 22 lists the following exemptions:

- *necessary for entering into, or performance of, a contract*;
- *authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests*; or
- *based on the data subject's explicit consent*.

Even if the refusal or limitation of a gaming account were interpreted to create a legal or similarly significant effect it is considered possible that, under certain circumstances, a form of profiling and/or solely automated processing could be used to determine the nature of a relationship with a player such as maximum stake, maximum deposit, review periods, etc. Reviewing the amount of new and existing accounts on this basis, and identifying trends which could signify problem gambling, is not practically possible for a human team. Therefore, automated processing for the initial contract, and any subsequent activity reviews, may be necessary for entering into and subsequent performance of a contract. The decision regarding whether such processing should be solely automated would be for the specific operator to identify.

h) To Contest the Decision and Seek Human Intervention

Whilst not described as a direct right under the GDPR, the safeguards that must be put in place around solely automated decision-making require operators to have a method for players to contest the decision and to require direct human review or intervention.

The process must be easily accessible by players and the operator's staff conducting any such review must be suitably skilled and appropriately senior to change the outcome if this is the conclusion of the review.

1.5) Principles for disclosing data to a third party

This chapter provides clarity and guidance on the principles for disclosing data to a third party. It includes but is not limited to the conditions for the sharing of personal data from an operator to a third party organisation, or organisations, in a data controller to data controller relationship. As the transmission from one operator to another clearly constitutes a disclosure to a third party, any transmission of data regarding the data portability right shall meet the requirements of this chapter. However, this chapter will not address disclosure of personal data between different parts of the operator's organisation, or the requirements for the disclosure of data to data processors as these topics are covered either by other parts of the Code or by the GDPR[13].

[13] See chapter 1.7 "relationships with processors and other controllers".

a) Compliance to GDPR

Any disclosure of personal data to a third party must comply with the Code and the GDPR. Regarding this chapter, each operator shall especially ensure adherence to the lawfulness of processing and transparency obligations.

b) Disclosure of personal data

By 'disclosure of personal data' the Code is referring to the sharing of personal data of players of an operator to any other organisation, regardless whether private or public. The Code covers the two main types of disclosure of personal data, to which different approaches apply:

- systematic / routine / repetitive disclosure of data;
- exceptional / non-routine disclosure of data.

c) Systematic disclosure of data

This will usually involve routine sharing of data sets between operators and third parties for a pre-arranged purpose. It could also involve a group of operators making an arrangement to pool their data for specific purposes. As this kind of disclosure will take place in a pre-planned and routine way, it shall be governed by established policies, or agreements, and processes to be determined by the operator. For example, this covers sharing data with regulatory authorities.

d) Exceptional disclosure of data

Operators may decide to, be asked or obliged to share data in situations which are not covered by routine procedures or agreements (e.g. police requests). In such situations, operators shall have policies and processes to be able to correctly determine whether or not the disclosure of data is in compliance with the GDPR and the Code.

One of the most important exceptional sharing practices is sharing personal data with sports bodies and other organizations involved in detecting match-fixing, self-betting and other sports or gambling related offenses/crimes. Some operators already have agreements in place for these sharing practices but even without such agreements, the legal basis for sharing the data is the public interest if provided in local law, in order to prevent and detect the crime or fraudulent activity, or alternatively, the legitimate interest of the operator. It is important that data is shared based on specific and detailed requests by the relevant body and that the operators share the minimum necessary data. Where this procedure is governed by law, operators will follow relevant law in regard to sharing the data with specific institutions. However, this does not preclude it to share with other bodies if that is in operator or other party's legitimate interests.

e) Transparency and Information

When disclosing player's data to third parties, operators shall make information on the recipients or categories of recipients of the personal data available to players at the time when personal data are obtained.

This information can be given by way of privacy policy[14]. The information shall be given in clear and plain language.

In certain circumstances operators can be legally obliged to refrain from informing the player of the disclosure of his data (like in the case of preventing and detecting crime).

To provide transparency even in said cases, the players shall be informed of the possibility and nature of such circumstances, if feasible, upon registration with the operator. This should be reflected in the privacy policy of the operator. In cases where prior information is not possible by any means, evidence of this fact shall be gathered and retained.

f) Documented Policies and Processes

These documents are the minimum required to satisfy the compliance with this part of the Code.

- Policy or process for the handling of personal data;
- Legitimate Interests Assessment methodology[15];
- Data Protection Impact Assessment methodology[16]; and
- Risk Assessment methodology.

All documents must be version controlled and must be reviewed and authorised at least annually. Where any of these documents are used to support a business decision, the appropriate version of that document must be referred to.

g) Policy or process for disclosure of personal data

The exact text of this policy does not form part of the Code. However, any implementation of it must contain the following information at a minimum in order to be compliant:

- A description of the methodology used regarding the decision to disclose or withhold;
- The technical and organisational measures information security controls around disclosure.

Furthermore, the operators shall gather and subsequently have readily available the information described in Art. 30 GDPR.

h) Security

[14] See chapter 1.4 "data subject rights".
[15] See chapter 1.3 "legitimate interests".
[16] See chapter 1.11 "Processing requiring Data protection impact assessments".

Operators shall take measures to facilitate the security of any disclosure of personal data to a third party. Operators shall choose the appropriate technical and organisational information security controls. Operators shall especially take into account the risks for the rights and freedoms of the players regarding the data to be disclosed. Where obliged by law to transfer personal data, the operator may have limited control over the security of the transfer[17].

1.6) Privacy by Design and by default

The GDPR has taken further the concepts of privacy by design and by default, formalising them into European law, requiring controllers to implement effective technical and organisational measures to ensure that the necessary safeguards and data protection principles are built into processes from the original concept stage and throughout the processing lifecycle. This means that any action an operator undertakes that involves processing personal data must be done with data protection and privacy in mind at every step, beginning with the initial design phase.

- Giving control of privacy to the players whose data is being processed through a user-friendly interface and default settings that respect the player's privacy;
- Giving players a choice about the processing of their personal data wherever possible (for example, by making it clear where the provision of data is voluntary or by making it easy for players to change their minds or withdraw consent, when processing was based on consent, without invalidating any prior processing which was based on consent).

Privacy by Design means proactively embedding privacy into the operations, system, infrastructure, and business practices. Operators under the Code pro-actively consider privacy and data protection throughout the lifecycle of their projects, which may include:

- Building new IT systems to process or access personal data;
- To comply with regulatory or contractual requirements;
- Developing new internal policies or strategies with privacy implications;
- Collaborating with an external party in a way that involves data sharing; or
- Using existing data for new purposes;
- Implementing a Data Protection Impact Assessment regime by conducting privacy impact assessment (PIA) or data protection impact assessment (DPIA) to identify and reduce data protection risks.

Privacy by design is aimed at the development of new systems, or changes to systems, that process personal data and as such, privacy by design is usually met through effective polices that will ensure the involvement of the DPO in every new or change of process related to processing personal data from the very beginning of this activity. Also, it can be met by carrying out a data protection impact assessment (but this is not necessary). However, this tool is not the only mechanism to achieve compliance with the GDPR and Art. 25 GDPR requires operators to cover both the technical and the

[17] See chapter 1.9 "security controls".

organisational aspects of ensuring compliance across their business – not just within the change management area. This means that operators should consider to implement actions in areas such as:

- Governance – leading from the top to develop a culture of awareness;
- Data protection risk management – identifying risks before they happen and establishing suitable controls;
- Having documented policies and procedures written in plain language to guide staff in how they need to handle the personal data they work with;
- Providing staff training and having performance management procedures;
- Documenting security standards that must be adopted across the business (including consideration of anonymization or pseudonymisation of personal data);
- Having mandatory controls around the appointment of processors who have access to personal data.

1.10) Personal Data Breach

One of the changes implemented by the GDPR relates to the mandatory notification of data breaches to the relevant SA. These new obligations are essential to the principles of accountability and transparency that run through the GDPR.

a) Definition of data breach and awareness

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, transmitted, stored or otherwise processed ("personal data breach"), where that personal data breach is likely to result in a high risk to the rights and freedoms of players, operators will ensure compliance with the requirements of Art. 33 GDPR.

a.1) Type of data breaches

The most used model for managing information security within an organisation is represented by the CIA triad of information security, which is centred in three key areas related to information systems, including Confidentiality, Integrity and Availability. Based on this model, under the Code personal data breaches can be classified in three different categories:

- Confidentiality breach: an unauthorised disclosure of, or access to personal data;
- Integrity breach: alteration or unauthorised changes of personal data;
- Availability breach: loss, accidental or unlawful destruction or loss of access to personal data.

A personal data breach could simultaneously affect the confidentiality, integrity and availability of personal data. In the online gambling sector, a loss of availability should be considered as a data breach. However, notification to the relevant SAs and the players concerned may not be necessary, if no confidential or integrity breach occurs and it has not a significant negative effect on players. For example, temporary loss of data that is properly encrypted and unintelligible for third parties would still be an availability breach. However, if the operator has any backup of the lost data, depending on the circumstances, it may or may not require notification.

Example of personal data breaches could include any of the following which lead to an impact on the personal data of the player:

- Loss or theft of data or equipment on which identifiable personal data is stored;
- Inappropriate access controls allowing unauthorised use;
- Equipment failure;
- Human error;
- Complete destruction of customer database;
- Unforeseen circumstances such as a fire or flood;
- A cyberattack that exposes names, addresses, dates of birth and encrypted passwords of players;
- Social engineering offences where information is obtained by deceiving the organisation who holds the records;
- Sending or disclosing personal data to an incorrect recipient;
- A significant disruption to the normal service of an operator due to power shutdown.

b) Notification

b.1) Detection

Under the GDPR, a new data breach notification regime will apply to mandate the reporting of certain personal data breaches to SAs and affected players, within 72 hours of becoming aware of the breach, where feasible.

Operators shall have in place a documented data breach response plan on dealing with a data security breach and take the appropriate steps deemed necessary to identify, contain and mitigate its possible adverse effects and resolve personal data breaches.

Such policy should include:

- The creation of a response team, which shall include at least the DPO or a member of their team, to prevent, identify, address and provide immediate and effective response to any unexpected event involving the unauthorised disclosure, loss or destruction of personal data;
- Responsibilities and authorities should be assigned to key individuals within the organisation;
- Procedures for establishing and communicating personal data breaches;
- Appropriate procedure of notifying the SAs and players of the personal data breach, if needed.

After becoming aware of a potential security incident, operators shall carry out a preliminary investigation in order to establish whether or not a breach has in fact occurred. During this period of investigation, operators may not be regarded as being “aware”. Operators will be considered “aware” of a breach, which initiates the 72 hours timeframe to notify the SA, as soon as it has a reasonable degree of certainty that a security incident has occurred and that personal data are compromised.

b.2) Containment

Once it has been established that a personal data breach has occurred, operators shall take immediate and appropriate action to limit the breach.

Operators shall evaluate:

- Who, within the organisation, needs to be made aware of the breach and inform them of what they are expected to do to contain the breach;
- Establish whether there is anything that can be done to recover any losses and limit the damage the breach can cause;
- Establish if it is appropriate to notify affected players immediately (e.g. where there is a high level of risk of serious harm to players); and
- Where appropriate (e.g. in cases involving criminal activities), inform the police.

If the remedial action is successful in preventing serious harm to affected players, the notification shall not be required.

b.3) Processors

The GDPR places direct obligations on data processors as well as data controllers. Data processors must report personal data breaches to operators without undue delay.
Operators and data processors should develop their internal breach notification procedures, including incident identification systems and incident response plans in order to ensure compliance with the legal timeframe. In cases where the data processing has been delegated to data processors, operators would be considered to be aware of a breach once the processor has become aware and operators have been notified.

Operators shall ensure that data protection clauses in contracts with their data processors are in place to define the processors' obligations during the duration of the contract. These clauses shall include that:

- Processors shall implement appropriate security measures to ensure personal data is secured;
- Processors shall proactively notify breaches to operators without undue delay;
- A duty to cooperate in "good faith" with the operators shall be incorporated to the contract to provide information of the data breach and the evaluation of risks to players as a result of a breach.

Reference is made to chapter 1.7.2 "Relationship with data processors".

c) Assessment

c.1) Risk

Operators shall have the obligation to report a personal data breach to SAs when the breach is likely to result in a residual risk to the rights and freedoms of players. When it is determined that a residual risk is high, the operator needs to notify both the SA and the affected players.

c.2) List of criteria to identify a high risk

To establish if a high risk exists, operator should check:

- if specific factors present high risks (e.g. the data contains login details, passwords or bank account details);
- whether the breach would cause any adverse effects for the players;
- how likely it is that adverse effects will materialise;
- whether the information has been disclosed to third parties; and
- if the intent of the breach was malicious.

c.3) Notification to Data Protection Authorities

Operators shall communicate with their lead SA as determined for the purposes of the "one stop shop".

The notification to SAs shall include:

- The nature of the personal data breach and a brief description of the incident;
- The categories and approximate number of players affected and personal data records concerned;
- The name and contact details of the DPO from whom more information can be obtained;
- The likely consequences of the personal data breach;
- The measures taken, or proposed to be taken, by the operator to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

In the event in which it is not possible to provide all the above information at the same time, operators will be able to provide information in phases without undue further delay. If the notification is delayed, operators will provide reasons for that delay by documenting why the delay in reporting is justified and not excessive.

d) Communication to players

Operators shall communicate to players, in plain language and in a simple manner, the existence of personal data breaches when it is likely to result in a "high risk" to their rights and freedoms.

The communication shall include:

- The nature of the breach;
- A description of the likely consequences;
- The measures that the operator has taken, or plans to take, to address and mitigate the breach;
- If possible, the operator should also provide practical advice to players on how to protect themselves from the consequences;
- The name and contact details of the DPO from whom more information can be obtained.

Operators will contact players individually directly by email, SMS or any other possible means. If such communication would involve a disproportionate effort, public communication should be used. The message should be accessible in alternative formats and relevant languages and, if possible, further information and recent updates should be available via the operators' website (where it is not possible to send message directly to the data subject) or directly communicated to the affected players.
For the communication to players, guidance from SAs, the EDPB and other bodies, such as law enforcement agencies, should be taken into account.

e) Accountability and record-keeping requirements for data breaches

Regardless of whether or not the personal data breaches need to be notified to the SA, operators shall keep a summary record of each personal data breach, which should enable the SA to verify compliance with the reporting and notification requirements under the GDPR.

The records must include:

- a chronology of the events leading up to the loss of control of the personal data;
- the amount and nature of the personal data that has been compromised;
- the action being taken to secure and / or recover the personal data that has been compromised;
- the action being taken to inform those affected by the incident or reasons for the decision not to do so;
- the action being taken to limit damage or distress to those affected by the incident; and
- the measures being taken to prevent repetition of the incident.

Where notification of a personal data breach to the relevant SAs has been made, such notification may be used as a record to satisfy the record-keeping requirement.

e.1) Responsibilities of Data Protection Officer regarding a breach

The responsibilities of the DPO can be described as:

- Making sure incident response plans, associated response and escalation procedures are defined and documented, to ensure that the handling of personal data breaches is timely and effective;
- Making sure that the personal data breach plan is up-to-date and reviewed;
- Collaborating in the investigation of a suspected or reported personal data breach and initiating the data breach response plan, as and when needed;
- Reporting to and liaising with external parties, legal representation, law enforcement, etc., as required;
- Authorising on-site investigations by appropriate law enforcement, as required during any security incident investigation. This includes authorising access to, or removal, of evidence from site;
- Notify and communicate personal data breaches to the relevant SA;
- Suggest action needed to be taken to reduce the risk of future breaches and minimise their impact;

- For each reportable personal data breach, a review and report shall be provided to the highest level of management.